附件 9

"网络空间安全治理"重点专项
2021 年度项目申报指南建议

（征求意见稿）

国家重点研发计划启动实施"网络空间安全治理"重点专项。本重点专项总体目标是：围绕全球网络公害、涉及民生的数据资产和"新基建"基础设施等领域的安全挑战，开展互联网基础设施、数据、网络公害、新技术新应用领域安全治理的战略性、基础性、前沿性研究，到 2025 年力争打造自立自强的网络空间安全治理技术体系，形成中国特色的网络空间安全治理方案，支撑实现网络空间的"共建、共治、共享"。

根据本重点专项工作部署，现提出 2021 年度项目申报指南建议。2021 年度指南部署坚持"需求牵引、问题导向、强化基础、引领前沿"的原则，拟围绕互联网基础设施治理、网络空间数据安全治理、网络公害治理及新技术新应用安全治理 4 个技术方向，启动 15 个指南任务。

1. 基础前沿类

1.1 抗量子计算的加密体系及安全机理研究

研究内容：针对量子计算对传统密码体系的威胁，研究公钥密码算法经典数学困难问题的传统计算和量子计算算法；研究抗量子计算公钥加密、密钥封装、密钥交换、数字

签名算法的设计理论与分析技术；研究抗量子计算密码算法的安全性；揭示对称密码算法组件抗量子计算攻击的安全机理，刻画抗量子计算对称密码算法的安全强度。

考核指标：密码算法在电子计算和量子计算下的安全强度不低于 128 比特，给出具体参数选取下密码算法的电子计算和量子计算下的安全强度；开发抗量子计算密码算法的开源库，抗量子密码算法≥10 个；申请国家发明专利≥20 件，其中国际专利≥3 件，获批行业以上标准立项≥3 项。

1.2 隐私计算及安全保障基础理论研究

研究内容：围绕建立体系化的隐私计算及安全保障理论，形成数据处理全流程的隐私保护能力，研究面向隐私信息采集、发布、共享等阶段的隐私计算及安全保障模型；研究多维度隐私信息形式化描述方法、隐私信息的智能感知技术；研究面向智能处理的、保护效果与数据可用性平衡的高效数据采集隐私保护技术；研究跨系统数据统计、查询、发布的隐私保护技术；研究隐私信息延伸控制、销毁与取证溯源监管机制；研究场景适应的隐私动态度量与隐私保护效果评估技术。

考核指标：提出不少于 5 类智能处理的数据采集本地差分隐私保护机制和信息率-失真隐私保护机制；提出不少于 5 类跨系统数据发布和查询统计的扰动、脱敏混淆等机制；提出跨系统转发行为的延伸控制和隐私侵犯行为的审计监管机制；开发隐私动态度量与保护效果评估工具集，支持不少

于5类的隐私保护算法保护效果进行评估。

1.3 面向去中心化网络的信任模型与密码算法研究

研究内容：针对去中心化网络中身份互认困难、共识性能要求高、核心密码算法缺乏设计与分析的问题，研究去中心化内生信任建立与跨域管理技术；研究去中心化网络共识机制设计与分析方法；研制去中心化网络节点身份管理系统；研究面向去中心化网络应用的加密算法和数字签名算法；研究去中化网络安全评估模型与主动动态防御方法。

考核指标：设计满足大规模去中心化节点信任管理的轻量级信任模型1个；提出至少1种新型节点共识算法，共识节点数超过200个，事务处理时延小于800ms；设计至少1种适用于去中心化网络的新型加密算法和数字签名算法，单核验签处理速度大于40000次每秒。

1.4 面向网络公害治理的知识图谱构建理论研究

研究内容：针对新型匿名化网络公害源头发现难、取证难、溯源难等问题，研究基于公害威胁数据时态特征的知识图谱构建方法；研究基于图挖掘的公害源关联分析方法；研究匿名网络公害行为主体画像及个体影响力分析技术；研究面向特定犯罪群体的画像追踪技术。

考核指标：实现1套数据规模在TB级别的公害威胁知识图谱系统，支持10种以上的异构数据输入，支持千万节点以上的图数据查询和机器学习处理，支持近实时的数据更新；匿名网络公害行为主体刻画准确度达到95%，主体行为

预测准确度达到 90%；特定群体犯罪预测成功率达到 80%。

1.5 人工智能安全防御及评估技术

研究内容：研究偏见等定向、非定向安全风险，设计面向数据和模型的检测、防御方法；设计对抗训练、网络蒸馏等人工智能模型防御方法；研究面向神经网络模型的复制、破坏、非法分发等手段；研究面向人工智能模型的安全性评估体系，研发模型的可信性、公平性、鲁棒性与可解释性评测工具。

考核指标：提出不少于 5 种针对分类器威胁的检测和防御方法、不少于 3 种面向数据和模型的去偏方法、不少于 5 种鲁棒性人工智能算法、不少于 3 种人工智能模型安全完整性认证和盗版溯源方法、不少于 5 种人工智能模型安全性评测方法；支持不少于 3 种常用开发框架、上亿级神经网络参数的规模化安全防御与评估。

2. 共性关键技术

2.1 纳米级芯片/硬件综合安全评估技术

研究内容：围绕纳米级处理器集成电路、微体系结构和芯片三个层面的硬件安全需求，研究芯片反向码点提取技术、微弱信号精准探测技术和 lowlevel 固件代码读取技术；研究处理器硬件脆弱性检测技术；研究具备验证权限正确性、数据完整性、信息私密性等的漏洞测评方法；研究能够与功能性电子设计自动化流程有效融合的安全验证方法及量化评估体系；研究面向白盒测试的芯片设计代码加速仿真

与设计结构安全检测。

考核指标：支持不少于5类国产自主研发制造和国外主流芯片厂商的处理器芯片的安全测试，支持对处理器微体系结构设计的批量形式化安全检测，支持基于硬件仿真模拟和形式化验证的检测手段；支持Verilog和VHDL两类设计语言的白盒测试加速仿真与设计结构安全检测，具备基于形式化模型实现设计中时间、能量和电磁侧信道检测的能力；芯片层反向码点提取技术支持纳米级空间分辨率、微弱信号精准探测技术支持微米级空间尺度和微秒级时间分辨率，lowlevel固件代码读取技术支持微米级空间电磁能力和亚微秒级时间分辨率。

2.2 互联网源地址验证表的分布式生成协议及设备研发

研究内容：针对当前互联网体系结构缺乏源地址验证体系的问题，研究自治域内部的源地址验证表分布式生成协议；研究自治域之间的源地址验证表分布式生成协议；研发高性能路由器，实现基于源地址验证表的源地址验证功能，实现源地址验证表的分布式生成协议。

考核指标：支持路由不对称和多路径路由场景下的源地址准确验证；自治域内部的源地址验证表生成协议支持路由环路检测；自治域之间的源地址验证表生成协议的通信开销不高于边界网关协议（BGP，Border Gateway Protocol）；提交IETF标准草案3项以上；路由器单槽位交换容量不低于1.8T，单机端口交换容量不低于36T。

2.3 高性能可扩展的资源公钥基础设施关键技术研究

研究内容：针对当前资源公钥基础设施（RPKI）存在的同步开销大、难以设置最长前缀长度、难以保障路径通告正确性等问题，研究 RPKI 的高性能数据同步方法，提高 RPKI 的可扩展性；研究 RPKI 最长前缀设置方法；研究 RPKI 根证书单边撤销的应急响应技术; 研究 RPKI 的路径验证技术; 研究 RPKI 的路由策略验证技术。

考核指标：RPKI 资料库支持依赖方在分钟级别增量同步所有资料库, 并保证依赖方对 RPKI 资料库视图的一致性; 最长前缀设置既能支持灵活的流量工程优化，又能防范子前缀劫持；提出降低 RPKI 对 5 个信任锚依赖程度的新技术，有效降低 RPKI 根证书单边撤销的风险；通过同时支持源验证、路径验证以及路由策略验证，RPKI 对 BGP 路由劫持和路由泄露的有效防范率达到 95%以上; 提交 IETF 标准草案 2 项以上。

2.4 开放环境下大数据安全利用研究

研究内容：针对当前开放环境中数据泄漏、恶意篡改、删除等问题，研究海量数据存储服务中的轻量级加密和安全存储理论，以及相应的安全高效存储、数据备份、高效数据同步技术；研究加密数据的高效安全检索技术，实现数据不解密情况下常用的数据检索操作；研究加密数据的高效计算技术，支持常用的数据运算操作；研究对平台数据、检索结果和计算结果的高效完整性认证技术；研究对开放平台的数

据滥用监管技术，提出针对开放计算平台数据滥用的有效监管。

考核指标：实现至少对 10TB 数据的高效存储、备份和同步运算；设计至少三种常用的加密数据计算方法，并在标准安全模型下证明其安全性；支持亿级数据量的存储、检索和计算，检索时间在秒级以下，并能对计算结果进行有效验证；实现存储、检索和计算的全日志功能，供第三方进行监管。

2.5 智能终端场景中移动应用的隐私管控研究

研究内容：针对智能终端场景中移动应用隐私保护与监管面临的底层安全支撑能力薄弱和运行时管控缺失难题，研究移动应用的数据敏感性量化及隐私保护效果评估方法；研究恶意应用和应用恶意收集数据行为的有效检测和准确溯源；研究从单一恶意应用检测到恶意应用家族检测以及恶意应用开发者、发布者和传播渠道的整体生态的安全性；研究应用运行时安全管控和威胁阻断技术；研发大规模移动应用隐私保护、管控和合规检测平台。

考核指标：研制一套大规模移动应用隐私保护和管控平台，支持日活亿级的移动设备管控；研制一套恶意应用家族检测系统和恶意应用开发者、发布渠道生态感知系统，支持不少于 20 种恶意应用家族；研发一套代码审计工具，能发现隐私和安全威胁不少于 10 种，数量不少于 20 个；在不少于三个现实业务场景开展应用示范。

2.6 隐私数据的个人权益保障研究

研究内容：针对个人数据被非法获取、交易和滥用等问题，研究个人敏感信息识别以及分类技术；研究公民个人采集信息的分散存储脱敏技术；研究针对个人敏感信息的监管技术；研究基于属性的个人信息保护和访问控制方法和理论，实现对个人信息扩散范围和使用期限的控制；研究数据遗忘技术，支撑公民对个人信息的遗忘权。

考核指标：支持至少 10 类以上不同人群个人敏感信息分类和识别，实现至少 100 万个个体敏感信息按照敏感级别进行分类；支持毫秒级的数据重构，支持至少对 100 万人的个人信息进行拆分脱敏存储和信息重构；研制一个个人敏感信息存储、管理和使用的综合性平台，提供对个人敏感信息监管服务、以及公民对个人信息的遗忘权和个人信息被使用的知情权等服务。

2.7 加密流量中网络公害检测与行为识别、阻断研究

研究内容：针对加密流量中网络公害监管与分析难、行为主体溯源难等问题，研究网络公害行为在加密流量各粒度层次下的形式表征方法；研究虚拟专用网络（VPN）网络流量的检测、工具识别；研究加密流量分类与网络公害行为识别方法；研究互联网加密网页、图片和视频内容真实性识别与验真技术；研究网络公害行为与主体的关联分析方法；研究面针对性网络公害行为流量阻断技术。

考核指标：VPN 流量识别时间不超过 20 秒，支持不少

于50种VPN工具分类；支持不少于20种常见加密应用分类，不少于5种网络公害行为分类与识别，时间不超过20秒，误报率小于10%，漏报率小于5%；实现网络公害行为与主体间的映射，主体数据库规模达千万级；支持常见加密视频平台不少于10种，能精准识别40万以上的视频，达到准确性不低于98%，误识率不高于1%，图片公害类型不少于5类，实现网络公害多媒体样本库规模不少于1000万条，公害账号库数据不少于10万。

2.8 智能驾驶汽车内部异构网络轻量化安全防护

研究内容: 针对智能驾驶汽车内部异构网络安全防护严重缺失，传统安全方案受计算、带宽等资源限制难以有效实施的问题，研究面向嵌入式ECU的轻量化身份认证、消息加解密及密钥协商安全算法，研究安全系统资源占用轻量化技术；突破安全数据载荷的轻量化技术，减少由安全数据引发的报文帧增多及报文数据位占用；研究车载网络不同功能区域的安全等级划分、分域隔离及车载网络专用防火墙技术。

考核指标: 车内时间敏感关键功能区域，数据加密处理与传输新增时延不超过5ms；安全防护相关应用占用运行内存不超过10%、占用存储空间不超过5%；安全数据载荷新增报文帧不超过10%、占用数据段不超过10%；车载网络支持多层级安全域划分，防火墙支持访问行为控制、危险操作阻断、可疑行为审计等；轻量化信息安全防护技术在不少于

3款车型上开展应用验证。

2.9 基于国产密码算法的工控编程平台安全防护技术

研究内容：围绕工控系统典型共性安全问题，研究工控安全防护模型，构建基于国产密码技术的工控编程平台安全防护框架；研究应用层代码、工程文件、操作记录、通信等加密技术；研究适配工业领域嵌入式平台运算能力的轻量级加密算法；研究编程平台应用层细粒度管控、运行态访问许可等认证技术；研究安全通信、静态可信认证、动态度量和身份认证体系。

考核指标：支持IEC61131-3规范，支持基于国产密码算法的标准总线协议栈加密，至少5种工业协议；可编程逻辑控制器(PLC)控制周期小于10ms，IO点数量大于1000点；支持不少于5种轻量级密码算法，性能不低于20Mbps；分散控制系统支持基于SM2、SM3、SM4的算法应用接口，支持通信加密、身份认证等功能，最小控制周期小于50ms，输入输出点数量大于10000点。

2.10 智能网联场景工业控制系统深度防御与安全处置技术

研究内容：围绕互联组网的智能装备集群对跨域跨时空网络威胁的有效应对、高安全弹性的防御架构以及强移动、强切换下的灵活性安全配置等的需求，研究面向智能装备互联场景的精细化网络管控技术；研究针对联网智能装备的高等级持续威胁联合协同分析技术；研究智能装备网络的安全

防御资源协同调度与灵活编排技术。

考核指标：支持5G网络可信接入，支持输入输出信号点10000点，控制周期20ms；支持至少3种工业控制系统网络检测，支持30种以上工业通讯协议监测，支持至少5类典型攻击异常监测报警；工控设备预警覆盖面达到80%，预警事件种类覆盖80%，预警诊断的准确率达到90%；支持至少3个行业的安全预警和应急响应方案；针对不少于2种重点行业在5G应用场景中开展应用验证。